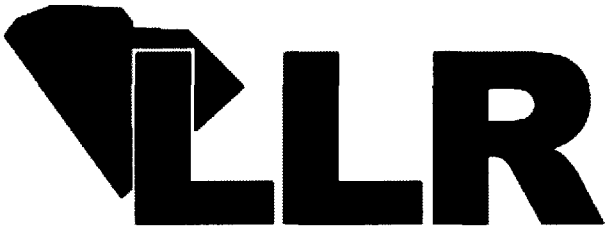
Remote Connection Improvement To SC OSHA OVP NCR Server



Chuck Combs
Information Resources Consultant
South Carolina Dept. of Labor, Licensing, and Regulation
110 Centerview Dr.
Columbia, SC 29210
Phone: 803-896-4343
E-mail: combsc@llr.sc.gov

CPM Project Paper
Submitted January 27th, 2004

Improve OVP remote connectivity to NCR Server

Introduction

In response to recent budget cuts the South Carolina Department of Labor, Licensing, and Regulation (LLR) needed to reduce costs. The Labor Division's facilities at 3600 Forest Drive in Columbia, South Carolina was closed and their offices were consolidated into LLR's headquarters located at 110 Centerview Drive in Columbia.

This consolidation made it necessary to greatly reduce the number of cubicles that were assigned to field personnel. As a result of these reductions most of the field people now work out of their homes and utilize a few common (shared) cubicles when they less frequently come into the main office.

The field personnel of the Office of Volunteer Programs (OVP) of the South Carolina's Occupational Health and Safety Administration (OSHA) must file reports on an old NCR server where the federal OSHA downloads the reports. The only remote access available for the field people is a single modem connection that will only allow one user at a time to be remotely connected. This restriction caused many of the field people to frequently work in the office to file their mandatory federal reports. Now there are not enough cubicles for the OVP field people to do this as they have in the past.

The OVP field personnel need improved remote access to their NCR server. This will allow them to file their reports more timely and with less frustration than they experience with a single modem connection access.

LLR's Office of Information Services (OIS) determined that there were three viable options to improve remote access to the OVP NCR server. These included adding additional modems to the NCR server, connecting over the

Internet through an open Internet port in LLR's firewall, and using the Internet to connect through LLR' virtual private network (VPN) switch.

The NCR server used by the South Carolina OVP is old and the federal OVP wants to take them out of service within the next year or two. Adding an additional modems and phone lines to the NCR server would still require out of town remote users to dial long distance to access the server. This would only allow one more person to log on at the same time on each modem installed using a different dial-up phone number.

A firewall is a computer hardware device with software running on it that controls the flow of network traffic into a protected network. The LLR firewall can be configured to pass Telnet Internet port traffic directly to and only to the NCR server.

LLR has a Nortel VPN switch in place and it is proven to be very secure with the use of encryption and key security. The Nortel VPN Client must be installed on each workstation and is the preferred method of connecting via the VPN switch. Each person that is to connect to the VPN switch must be setup in the switch security configuration.

Security, costs, ease of use, and difficulty of implementation must be considered to determine the best approach to improve OVP's remote access to their NCR server.

Modem connections and VPN connections have been in use for several years in LLR and are acceptably secure. The security of Telnet connections through an open Internet port in a firewall must be determined.

There are no additional costs for either of the Internet options so the costs of adding additional modems and analog phone lines must be obtained.

The use of the modem connection is the easiest to use and the direct Internet connection through the firewall would only be slightly harder for the users. The use of a VPN connection has one more additional step to establish the secure connection, which makes it slightly harder.

Installing additional modems on the NCR server would not require LLR's support staff to do anything since the federal OVP would do that. Only minor workstation and firewall configuration changes would be needed to connect through an open Internet port in LLR's firewall. To connect to LLR's VPN switch a small client program would need to be installed on each workstation and each user would be need to be setup in LLR's VPN switch.

Information Sources

Since the NCR server is a federal OVP controlled server, several requests have been made for information about the costs of adding additional modems. The costs for analog data lines will be obtained from LLR's Procurement office.

The security of a remote Telnet connection passing through the LLR firewall can be researched through web based technical articles and publications, consulting with information technology consultants in other agencies, and brainstorming with LLR Information Resources Consultants with knowledge of Internet protocols and firewall configurations. A web search was made for Telnet security. The following are a few of the articles that were found:

Title: Please use Secure Shell instead of Telnet or rsh/rcp/rlogin
By: Vassar College, Poughkeepsie, New York – Dept. of Physics and Astronomy
Link: http://noether.vassar.edu/~myers/help/SecureShell.html

Title: Secure Shell (SSH): Answers to Frequently Asked Questions (FAQ)
By: Princeton University Office of Information Technology

Link: http://helpdesk.princeton.edu/kb/display.plx?id=2748

Title: Personal Computer and Information Security Best Practices
By: Paul F. Troncone - Polytechnic University
Link: http://pangea.stanford.edu/computerinfo/pangea/faq/connection.html

All the information that is obtained will be reviewed and discussed with LLR's Information Resources Consultants and the managers of the OVP field staff. Data security will have the highest priority in any decisions made. The group will consider costs, ease of use, and difficulty of installation with lesser importance.

Results

As of this date the federal OVP has not responded to requests for the costs of adding additional modems. The NCR system is so old that the federal OVP now contracts the support out and the contract is only in place for one more year. The manufacturer of the existing modem is no longer in business but a web search found that a single modem originally cost approximately $450 and used ones could be purchased for $100. The cost of a single analog modem line is $12.55 per month.

In initial brainstorming sessions, LLR's Information Resources Consultants considered good ways to remotely connect to the OVP NCR server. They determined that the existing modem connection, the easiest way to allow the OVP field folks to connect to their NCR server would be to connect directly by passing through an open Internet port in the LLR firewall. The firewall could be configured to only pass the Telnet Internet port traffic and only pass it to the OVP NCR server. This would just require a special configuration on the firewall and changing the Internet address on the remote computer's Telnet client – both changes being fairly simple. It was decided though that we should research the security of the Telnet connection over the Internet.

During the initial brainstorming session it was also decided that the only other Internet option that should be considered to remotely connect would be using a Nortel VPN client to make a secure encrypted connection to LLR's Nortel VPN switch. This decision was made due to their being no cost to use the Nortel software and that it is known to be secure since it establishes a secure encrypted tunnel between the remote workstation and the LLR VPN switch.

In meetings with the manager of LLR's OVP section, their computer liaison, and one of the more technically skilled field people, they again pointed out that their main source of frustration is the current single modem dial-up connection that only allows one remote user at a time to connect and use the NCR server. It was explained to them that there were only three options that we (LLR's information technologies department) wanted to consider. Two of the three options are the access via the Internet discussed above and the third option being the addition of additional modems and phone lines to allow more users to be simultaneously connected to the NCR server. The OVP people stated that dialing in remotely from out of town locations created long distance phone charges. They also said that most of their field people had personal Internet connections that they would be willing to use to access the NCR server. Since using the Internet would be faster and would allow all their remote connections to connect at the same time, they said using the Internet would be preferred over adding additional phone lines and modems. Since it was probable that the NCR system would be replaced in the near future it was decided to not further pursue the option of adding additional modems to the NCR server.

In discussions about remote connections over the Internet, Justin Ellis (LLR Information Resources Consultant) suggested that we contact Eric Hamberg who is an Information Resources Consultant at the South Carolina Employment Security Commission (ESC). Justin who recently came from ESC worked with Eric Hamberg and knew that he worked extensively the remote connections in

much larger agency with many remote sites. Eric quickly stated that Telnet is not secure because it passes usernames and passwords as plain text, which can be captured by hackers. He said that there were more secure encrypted methods that should be used.

To verify what ESC's Eric Hamberg told us, a web search was done on Telnet security and hundreds of the sites found supported the fact that Telnet passed usernames and password as unencrypted plain text. Three of the more reputable web sites are listed in the Information Sources section above. It was found that a large majority of corporate and agency networks do not allow native Telnet connections any more due to the lack of encryption. Many of the websites promoted the use of newer encrypted applications instead of using the generic Telnet.

LLR's Justin Ellis used a network security and vulnerability program (Retina) to scan the NCR server. The Retina program reported that the NCR server was not secure because Telnet was enabled. It was further found that the old NCR server did not have other security features that could improve Telnet security.

Summary

This project was to determine the best way to improve remote connectivity to an old NCR server for LLR's OVP field people. Three options were considered viable and were researched. These options included adding additional modems to the NCR server, directly connecting over the Internet passing through an open Internet port on the LLR firewall, and connecting over the Internet using LLR's Nortel VPN switch.

Adding additional modems and phone lines to the NCR was the only option that would have required any monetary expenses. When the federal OVP group was asked for cost estimates to add additional modems it was found that they are

actively looking at replacing the NCR server with a server running a Microsoft Windows Server operating system. The age and obsolescence of the old NCR server and existing modems made it difficult to obtain significant information on them. This option was eliminated because of the questionable life of the existing NCR server and only one additional person could connect simultaneously for each modem added.

Using an existing Telnet client to connect directly to the NCR server over the Internet and through an open port in LLR's firewall was eliminated for security reasons. This option was eliminated because it passed usernames and passwords as unencrypted plain text. New encrypted applications like Telnet are available but at a cost and they would have probably required an upgrade to the obsolete NCR server.

The third and chosen option was using the Internet to connect to LLR's VPN switch. Once the secure tunnel connection is made, the existing Telnet client can be used to connect to the NCR server. This was the only option that did not require any research because it has been in use for two years and has proven to work securely. It will require adding the additional free Nortel VPN client to each computer that is to remotely connect to the NCR server.

Conclusions

Security, costs, ease of use, and difficulty of implementation were the primary considerations for this project. The differences in costs, ease of use, and difficulty of implementation were considered to be relatively small.

Security was the highest consideration on this project. The connection directly to the NCR server through an open Internet port in LLR's firewall would have been the easiest option to get up and running but it was found to not be secure. A

VPN connection establishes a secure encrypted tunnel in which the workstations can securely communicate with the NCR server.

The final choice was a very obvious choice. It was not obvious until after it was determined that the old NCR system was found to be so obsolete that the federal OVP is moving to replace it. What was first known to be the easiest way to remotely connect over the Internet was then found to not be secure in today's Internet environment. Telnet has been used for years and in the past was considered secure because remote users had to log in with a username and password. Hacker technology has progressed and will they will continue to seek and achieve ways to exploit vulnerabilities in computers and networks. The computer industry continues to remove and patch those vulnerabilities to protect the information that is stored and transferred from one system to another.

Further Recommendations

This project will be considered a success when the OVP field people have sufficient remote access to their NCR server to eliminate their connection frustrations. All those that do not have home Internet access or chose not to use it, will continue to share the dialup connection which should be sufficient for the reduced number of users. When all the OVP field people that want the remote connection to the NCR server through their home Internet service have been setup this project will be completed.

The results of this project have brought a new awareness of the vulnerabilities of Telnet connections. With this information LLR's Office of Information Systems should look into the security of Telnet connections to the agency's AS400 midrange computer.